Datenschutz im vernetzten Automobil

Benedikt Buchner

Angaben zur Veröffentlichung / Publication details:

Buchner, Benedikt. 2015. "Datenschutz im vernetzten Automobil." *Datenschutz und Datensicherheit - DuD* 39 (6): 372–77. https://doi.org/10.1007/s11623-015-0432-6.

Benedikt Buchner

Datenschutz im vernetzten Automobil

Die Vernetzung des Automobils eröffnet eine neue Chance aufzuzeigen, dass moderne Technik und effektiver Datenschutz keineswegs unvereinbare Gegensätze sein müssen. Es besteht die Gelegenheit, ein Gegenmodell zum datenschutzignoranten Geschäfts- und Ideenmodell des Silicon Valley zu entwerfen – ein Gegenmodell, welches Technik gleichermaßen rechtskonform wie nutzerfreundlich ausgestaltet. Einige wenige Eckpunkte für ein solches Modell sollen im Folgenden angedacht werden.

1 Ausgangspunkt

Eine besondere datenschutzrechtliche Herausforderung beim vernetzten Automobil ist die Ausgestaltung der Rechtsbeziehungen zwischen den verschiedensten Akteuren: auf der einen Seite Hersteller, Händler, Plattformbetreiber, Drittanbieter usw. und auf der anderen Seite Fahrzeughalter, Fahrer und Beifahrer, mitunter noch in Sonderrollen als Beschäftigte, Versicherungsnehmer etc.[1] Wie auch sonst im Datenschutzrecht ist dabei vor allem die Einwilligung des Betroffenen in eine Datenverarbeitung von zentraler Bedeutung.

1.1 Das Hohelied auf die Transparenz

Eine Maxime, die von allen gleichermaßen hochgehalten wird, wenn es um die Ausgestaltung der Rechtsbeziehungen zwischen den Beteiligten geht, ist der Grundsatz der Transparenz. Entsprechend zieht sich diese Vorgabe der Transparenz wie ein roter Faden durch das gesamte Datenschutzrecht. Das BDSG ist voll mit Informationspflichten, die für den Betroffenen eine Transparenz der Datenverarbeitung gewährleisten sollen.[2] Das TMG setzt diese Linie fort und normiert nochmals eine Vielzahl spezifischer Informationspflichten für den Telemedienbereich.[3] Exemplarisch hierfür steht § 13 Abs. 1 Satz 1 TMG, wonach Diensteanbieter „den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb [Europas] in allgemein verständlicher Form zu unterrichten“ haben.

So einleuchtend und erstrebenswert eine solcherart normierte Transparenz ist, so ernüchternd ist die konkrete Umsetzung dieses Leitgedankens bis dato in der Praxis. Wer einen Eindruck davon bekommen möchte, was Diensteanbieter in der Online-Welt unter Transparenz verstehen, dem sei ein Studium der von Facebook zur Verfügung gestellten Informationen empfohlen. Wer sich im Sinne von § 13 Abs. 1 TMG „über Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten“ bei Facebook in dessen AGB, Datenverwendungs- und Cookie-Richtlinien informieren möchte, kann sich zu diesem Zweck immerhin umgerechnet 19 DIN A 4-Seiten zu Gemüte führen. Wer sie sorgfältig liest, wird dann u. a. auch den Hinweis finden, dass für sog. Facebook-Unternehmen wie Instagram oder WhatsApp wiederum eigene Datenschutzrichtlinien und Nutzungsbedingungen gelten, die ebenfalls zu beachten sind.[4] Und für den – alles andere als ungewöhnlichen – Fall, dass der Nutzer weitere Apps, Webseiten oder sonstige Dienstleistungen verwendet, sind dann zusätzlich auch noch die Bedingungen und Richtlinien des jeweiligen Anbieters dieser Apps, Webseiten etc. einschlägig. Stellt man zudem in Rechnung, dass sich all diese Richtlinien, Policies und Klauselwerke ständig ändern, kann man kaum noch ernsthaft behaupten, dass eine auf solche Weise gehandhabte Transparenz noch etwas mit einer tatsächlichen Informiertheit seitens der Telemediennutzer zu tun hat. Tatsächlich handelt es sich um ein klassisches Beispiel des Information overload, Diensteanbieter beschränken sich allein darauf, formal korrekt ihre Informationspflichten abzuarbeiten.

Verfolgt man die gegenwärtige Diskussion um den Datenschutz im Automobilbereich, kann man den Eindruck gewinnen, dass auch hier wieder überhöhte Erwartungen an das vermeintliche Erfolgsrezept der Transparenz geknüpft werden. Fast schon in wörtlicher Anlehnung an § 13 Abs. 1 TMG lautet eine der Emp-

1 Ausführlich zu den zahlreichen Akteuren *Roßnagel* (in diesem Heft).

2 Siehe nur für die Direkterhebung beim Betroffenen § 4 Abs. 3 BDSG, für die Datenverarbeitung durch öffentliche Stellen § 19 BDSG, für nicht-öffentliche Stellen § 34 BDSG und § 42a BDSG bei unrechtmäßiger Kenntniserlangung von Daten.

3 Bereits die §§ 5 und 6 TMG normieren – noch ohne spezifischen Bezug zum Datenschutz – zahlreiche allgemeine und besondere Informationspflichten für Diensteanbieter. Ergänzt werden diese durch eine Vielzahl von Informationspflichten im datenschutzrechtlichen Regelungsabschnitt: § 13 Abs. 1 und 7 TMG und § 15a TMG.

4 Beim Beispiel WhatsApp sind das immerhin weitere 13 Seiten an AGBs und Datenschutzrichtlinien.

Prof. Dr. Benedikt Buchner, LL.M. (UCLA)

Direktor des Instituts für Informations-, Gesundheits- und Medizinrecht (IGMR), Universität Bremen

E-Mail: bbuchner@uni-bremen.de

fehlungen des 52. Deutschen Verkehrsgerichtstags[5], dass Fahrzeughersteller und weitere Dienstleister „Käufer bei Vertragsabschluss in dokumentierter Form umfassend und verständlich informieren [müssen], welche Daten generiert und verarbeitet werden sowie welche Daten auf welchen Wegen und zu welchen Zwecken übermittelt werden." Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder mahnt für Fahrer, Halter und Nutzer von Fahrzeugen „vollständige Transparenz" an; gefordert wird, dass diese „umfassend und verständlich darüber zu informieren sind, welche Daten beim Betrieb des Fahrzeugs erfasst und verarbeitet sowie welche Daten an welchen Schnittstellen an wen und zu welchen Zwecken übermittelt werden."[6] Mit Blick auf die Erfahrungen im Telemedienbereich stellt sich die Frage, wie realistisch solcherlei Transparenzforderungen für den Automobilbereich sind. Wenn schon die Komplexität der Datenverarbeitung bei Computern und Smartphones eine echte Transparenz in weite Ferne rücken lässt, ist nur schwer vorstellbar, wie die nochmals komplexeren Datenverarbeitungsprozesse beim „Smartphone mit Rädern"[7] transparent darstellbar sein sollen.

1.2 Abgestufte Herangehensweise

Möchte man der bis dato zu verzeichnenden und auch zukünftig zu befürchtenden Informationsflut Herr werden, bietet sich in einem ersten Schritt zunächst einmal eine abgestufte Herangehensweise an. Eine erfolgreiche Umsetzung der Transparenzidee scheitert bislang auch daran, dass Informationen zu undifferenziert präsentiert werden. Nicht alle Informationen über das Ob und Wie einer Verarbeitung personenbezogener Daten sind gleichermaßen von Relevanz. So mag für manchen zwar auch interessant sein, ob und wie Daten auf gesetzlicher Grundlage verarbeitet werden. Für die Ausgestaltung der Rechtsbeziehungen zwischen Betroffenem und Datenverarbeiter sind solcherlei Informationen jedoch irrelevant. Transparent müssen insoweit nur diejenigen Rahmenbedingungen sein, die der Betroffene kennen muss, um sich für oder gegen die Einwilligung in eine Verarbeitung seiner personenbezogenen Daten entscheiden zu können.

Was hingegen ohnehin gesetzlich erlaubt ist und daher dem Betroffenen keine informierte Entscheidungsfindung abverlangt, hat im *gestaltenden* Teil der Rechtsbeziehungen zwischen den Beteiligten nichts verloren.[8] Vielmehr reicht es aus, dass solcherlei Informationen dem interessierten Leser in einer Art von „Begleitlektüre" (Benutzerhandbuch, Driver's Guide o.Ä.) mitgeteilt werden. Im Zuge seiner Entscheidungsfindung sollte es dem einzelnen Betroffenen soweit wie möglich erspart bleiben, sich auch noch mit solchen Datenverarbeitungsprozessen auseinandersetzen zu müssen, die bereits gesetzlich erlaubt sind, weil sie der Sache nach ohnehin geboten sind und weder die Interessen der einen noch der anderen Seite nennenswert berühren. Dies gilt etwa für solche Standarddatenverarbeitungsprozesse wie die Verarbeitung von Nutzungsdaten für Abrechnungszwecke oder die Datenspeicherung zum Zwecke der technischen Nachrichtenübermittlung, wie sie für den Telekommunikations-, Multimedien- und Telemedienbereich mitunter sehr detailliert normiert sind. Im Sinne einer effizienten Arbeitsteilung ist es sachgerecht, wenn insoweit der Gesetzgeber solche – regelmäßig kaum interessenrelevanten – Details der Datenverarbeitung regelt, während die Beteiligten ihre Zeit und Energie auf die Gestaltung derjenigen Rahmenbedingungen konzentrieren können, die die eigentlich datenschutzrelevanten Fragestellungen betreffen.[9]

Erst recht irrelevant für den Prozess der Willensbildung sind (zumindest aus datenschutzrechtlicher Perspektive) solche Datenverarbeitungsprozesse, die sich auf Daten *ohne Personenbezug* erstrecken. Auch insoweit gilt, dass dahingehende Informationen im *gestaltenden* Teil der Rechtsbeziehungen nichts zu suchen haben, sondern allenfalls in der „Begleitlektüre". Im Ergebnis gilt daher, dass jede Ausgestaltung der Rechtsbeziehungen zwischen den Beteiligten, die sich ernsthaft um Transparenz bemüht, vorweg diese beiden Fragestellungen klären muss: Inwieweit kommt es überhaupt zu einer Verarbeitung *personenbezogener* Daten? Und, soweit dies der Fall ist: Welche (datenschutzrelevanten) Verarbeitungsprozesse sind bereits *auf gesetzlicher Grundlage zulässig* und bedürfen daher keiner individuellen Einwilligung des Betroffenen mehr?

2 Personenbezogene versus fahrzeugbezogene Daten

Die Frage der Personenbeziehbarkeit von Daten wird im Fall des vernetzten Kraftfahrzeugs oftmals unter dem Aspekt „personenbezogene versus fahrzeugbezogene Daten" thematisiert.[10]

Unstreitig ist, dass eine Vielzahl von Daten, die im Zuge der Kfz-Nutzung anfallen (Betriebs-, Komfort-, Fehler- und Wartungsdaten) im Ausgangspunkt zunächst einmal technische Daten des Fahrzeugs sind, die dessen Betrieb, Fehlerfreiheit und Sicherheit gewährleisten sollen. Andererseits sind Daten über ein Fahrzeug potenziell stets auch Daten über dessen Fahrer bzw. Halter.[11] Sie liefern beispielsweise Informationen über den Umgang mit dem Fahrzeug, wenn es um Fragen der Gewährleistung geht. Oder sie liefern Informationen über das Fahrverhalten, wenn es um Versicherungstarife oder die Schuldfrage in einem Unfall geht usw. Der Verweis, die Personenbeziehbarkeit von Fahrzeugdaten sei „im Einzelfall nur im Fall des Hinzutretens weiterer Ereignisse oder besonderer Umstände von Bedeutung (bspw. im Fall eines schweren Unfalls)", ist in diesem Zusammenhang kein Argument gegen, sondern für eine Einordnung der Fahrzeugdaten auch als personenbezogene Daten.[12]

Gleichwohl würde es andererseits zu weit gehen, sämtliche fahrzeugbezogene Daten stets auch differenzierungslos als perso-

5 52. Deutscher Verkehrsgerichtstag 2014, Empfehlung Arbeitskreis VII (Wem gehören die Fahrzeugdaten?), Ziffer 2.

6 DuD 2015, 44 („Datenschutz im Kraftfahrzeug – Automobilindustrie gefordert").

7 *Weichert,* Datenschutz im Auto, 52. Deutscher Verkehrsgerichtstag (2014), S. 285.

8 Allgemein zur Unterscheidung zwischen (verbindlichen) Vertragsbedingungen einerseits und bloßen Hinweisen ohne eigenständigen Regelungsgehalt andererseits siehe etwa BGH NJW 2009, 1337.

9 Vgl. *Buchner,* Informationelle Selbstbestimmung im Privatrecht (2006), S. 175.

10 Siehe bspw. bei *Kinast/Kühnl*, NJW 2014, 3057.

11 Ausführlich zu den verschiedensten Arten von Daten, die im vernetzten Kfz anfallen, die Beiträge von *Hansen* sowie von *Krauß/Waidner* (in diesem Heft).

12 Nicht so recht klar wird demgegenüber, welche Konsequenzen die Bundesregierung aus diesem Umstand ziehen möchte, insbesondere wenn es dann im Folgenden heißt, dass angesichts dieser Ausgangslage „die faktische Bedeutung einer Herstellung des Personenbezuges im Alltag der Fahrzeugnutzer eingeschränkt" sei; siehe Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Renate Künast u. a., Datenschutz im Auto, Ziffer 11 (BT-Drucksache 18/1362).

nenbezogene Daten zu behandeln.[13] So sind insbesondere all diejenigen Daten datenschutzrechtlich irrelevant, die „flüchtig" sind, weil sie schon aus Gründen der Speicherkapazität nicht längerfristig gespeichert, sondern fortlaufend gelöscht bzw. überschrieben werden. Was das Bundesverwaltungsgericht erst jüngst als Richtschnur für die automatisierte Erfassung von Kraftfahrzeugkennzeichen entwickelt hat, kann entsprechend auch als Differenzierungskriterium für die fahrzeuginterne Erfassung von technischen Daten herangezogen werden: Datenschutzrechtlich irrelevant sind danach Datenerfassungen stets dann, wenn die Daten „unmittelbar nach der Erfassung technisch wieder spurenlos, anonym und ohne die Möglichkeit, einen Personenbezug herzustellen, ausgesondert werden."[14] Vorzunehmen ist nach dem Bundesverwaltungsgericht eine Gesamtbetrachtung, maßgeblich soll sein, ob mit Blick auf den durch den Verwendungszweck bestimmten Zusammenhang sich das „Interesse an den betroffenen Daten bereits derart verdichtet hat, dass ein Betroffensein in einer einen Grundrechtseingriff auslösenden Qualität zu bejahen ist".[15] Damit gilt: Im Fahrzeug erhobene Daten können stets dann als bloße technische und fahrzeugbezogene Daten eingeordnet werden, wenn diese nur punktuell erhoben werden, um entsprechende Fahrzeugfunktionen zu ermöglichen, und technisch gesichert ist, dass die Daten sodann sofort spurenlos wieder gelöscht werden, ohne dass die Möglichkeit besteht, einen Personenbezug herzustellen.[16]

Datenschutzrechtlich irrelevant sind auch alle Verarbeitungsprozesse, die sich auf die Nutzung anonymisierter Daten beschränken. Daten, die sich i. S. d. § 3 Abs. 6 BDSG „nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft" einer Person zuordnen lassen, sind nicht mehr personenbezogen im datenschutzrechtlichen Sinne.[17] Grundsätzlich gilt dies auch für alle Datendienste im vernetzten Auto, soweit eine anonyme Nutzung dieser Dienste technisch gewährleistet wird. Fraglich ist allerdings, ob sich in Zeiten von Big Data eine Differenzierung von anonymisiert einerseits und personenbezogen andererseits überhaupt noch dauerhaft aufrechterhalten lässt, zumindest, wenn es sich nicht nur um bloße statistische Daten handelt, sondern um Daten zu einer individuellen (lediglich nicht „bestimmbaren") Person. Wenn für die anonymisierten Kreditkartendatensätze von 1,1 Millionen Menschen gilt, dass hier mit relativ wenig Aufwand einzelne Menschen herausgefiltert werden können,[18] so ist davon auszugehen, dass Gleiches auch bei anonymisierten Bewegungsprofilen, Nutzungsprofilen u.Ä. möglich ist. Je weiter Big Data voranschreitet, desto geringer wird der „Aufwand an Zeit, Kosten, Arbeitskraft" i. S. v. § 3 Abs. 6 BDSG ausfallen, um an sich anonymisierte Daten gleichwohl einer Person zuordnen zu können bzw. umso höher sind die Anforderungen an technische Speicherkonzepte, um eine dauerhafte Anonymisierung von Daten annehmen zu können.

Egal auf welche Weise eine Spurenlosigkeit von technischen oder sonstigen Daten gewährleistet werden kann – ob durch verlässliche Anonymisierung oder sonstige Lösch- und Speicherkonzepte – genutzt werden sollten solcherlei Möglichkeiten in jedem Fall, nicht nur im Sinne der Datensparsamkeit, sondern auch mit Blick auf eine betroffenenfreundliche Ausgestaltung der Rechtsbeziehung zwischen den Beteiligten. Je weniger personenbezogene Daten anfallen, desto schlanker können Verträge gehalten werden und desto eher ist es möglich, die Aufmerksamkeit auf diejenigen Datenschutzfragen zu lenken, die im Verhältnis von Datenverarbeitern und Betroffenen tatsächlich gestaltungsbedürftig sind.

3 Gesetzliche Erlaubnistatbestände

Weisen die Daten, die im Zuge einer Kfz-Nutzung verarbeitet werden, einen Personenbezug auf, so greift das datenschutzrechtliche Verbotsprinzip mit Erlaubnisvorbehalt, die Datenverarbeitung bedarf daher, um zulässig zu sein, entweder einer gesetzlichen Erlaubnis oder muss auf eine Einwilligung des Betroffenen gestützt sein. Damit sich – im Sinne der Transparenz – die Beteiligten im gestaltenden Teil ihrer Rechtsbeziehungen auch tatsächlich auf die Datenverarbeitungsvorgänge konzentrieren können, die eines privatautonomen Aushandelns (Einwilligung) bedürfen, müssen zuvor entsprechend die Datenverarbeitungsprozesse abgeschichtet werden, die bereits auf gesetzlicher Grundlage erlaubt sind. Hierfür wiederum ist zunächst einmal zu klären, welche Gesetze (i.e.L. BDSG, TMG, TKG) beim vernetzten Fahrzeug überhaupt einschlägig sind.

3.1 Kommunikationsdaten: TMG?

Kfz-Kommunikationsdienste sollen „praktisch durchgehend" als Telemediendienste einzustufen und ihre Zulässigkeit entsprechend nach dem TMG zu beurteilen sein.[19] Zutreffend ist dies sicherlich für all die Konstellationen, in denen das „Internet ins Fahrzeug" geholt wird, die elektronischen Informations- und Kommunikationsdienste i. S. v. § 1 TMG also nicht über Laptop oder Smartphone, sondern stattdessen über die Bedieneinheit im Auto genutzt werden.

Fraglich ist demgegenüber, ob und in welchen Konstellationen das TMG auch gilt, wenn nicht das „Internet ins Fahrzeug", sondern umgekehrt das „Fahrzeug ins Internet" geholt wird (z.B. um einen Fernzugriff auf das Fahrzeug zu ermöglichen). Die gleiche Frage stellt sich, wenn es um Car-to-X bzw. Car-to-Car-Kommunikation geht (etwa zu Verkehrsinformations- oder Warnzwecken). Derlei Kommunikationsvorgänge haben mit den typischen Telemediendiensten, wie sie der Gesetzgeber bei Verabschiedung des TMG vor Augen hatte,[20] nur wenig gemein; die besseren Gründe sprechen hier für eine Anwendbarkeit des BDSG. Abzulehnen ist eine Einordnung als Telemediendienst jedenfalls dann, wenn die kommunizierten Inhalte vom einzelnen Nutzer gar nicht mehr wahrgenommen werden, weil die Kommunikation unmittelbar zwischen den Fahrzeugsystemen selbst stattfindet und Informationen ohne Einbindung des Fahrers direkt weiter-

13 A.A. *Kinast/Kühnl*, NJW 2014, 3057, 3058, die auch rein fahrzeugbezogene Daten vom Anwendungsbereich der Datenschutzgesetze erfasst sehen.

14 BVerwG DuD 2015, 196, 198 mit Verweis auf BVerfG v. 11.3.2008 (DuD 2008, 352).

15 BVerwG a.a.O.

16 Zu entsprechenden Speicher- und Löschkonzepten siehe den Beitrag von *Rieß/Greß* (in diesem Heft).

17 *Tinnefeld/Buchner/Petri*, Einführung in das Datenschutzrecht (5. Auflage 2012), S. 228.

18 Ausreichend hierfür war in der konkreten Untersuchung die Kenntnis von lediglich vier Bezahlvorgängen einer bestimmten Person, welche dann mit dem Datensatz abgeglichen wurden. In 90% der Fälle ließ sich die betreffende Person sodann in dem Datensatz wiederfinden; Süddeutsche Zeitung vom 29.1.2015 („Anonymisierte Datensätze nicht so sicher wie gedacht").

19 Siehe *Weichert,* a.a.O., S. 288.

20 Vgl. dazu BT-Drucksache 16/3078, S. 13.

verarbeitet werden.[21] Nicht in den Anwendungsbereich des TMG fallen darüber hinaus auch alle technischen Daten wie Betriebs-, Komfort- oder Fehler- und Wartungsdaten, die im Fahrzeug erzeugt werden.

3.2 Inhaltsdaten: BDSG?

Die Anwendbarkeit des BDSG (statt TMG oder TKG) wird vor allem auch davon abhängig gemacht, um welche Art von Daten es sich handelt, die verarbeitet werden. So soll für sog. Bestandsdaten sowie Nutzungs- bzw. Verkehrsdaten das TMG bzw. TKG einschlägig sein, für sog. Inhaltsdaten demgegenüber das BDSG gelten.[22] Im Telemedienbereich werden zu diesen Inhaltsdaten regelmäßig diejenigen Daten gezählt, die zwar auch online ausgetauscht werden, die allerdings mit der Ausgestaltung sowie mit der ordnungsgemäßen Erbringung und Abrechnung eines Telemediendienstes unmittelbar nichts mehr zu tun haben, sondern lediglich „aus Anlass" eines Anbieter-Nutzer-Verhältnisses i. S. d. TMG anfallen (beispielsweise die Daten zu einem Buchkauf über einen Online-Anbieter oder das Erstellen einer Profilseite in einem sozialen Netzwerk).[23] Auch für die Datenverarbeitung beim vernetzten Kfz soll wieder eine solche Differenzierung nach verschiedenen Datenkategorien gelten.[24]

Jedoch stellt sich – wie schon für den Telemedienbereich[25] – auch für den Kfz-Bereich die Frage, ob eine solche Differenzierung wirklich zielführend ist. Gegen eine solche Differenzierung spricht bereits, dass eine Grenzziehung zwischen Nutzungs- und Inhaltsdaten in vielen Konstellationen mehr oder weniger willkürlich ausfällt. Es ist auch kein Grund ersichtlich, warum ein einheitlicher Lebenssachverhalt, egal, ob es die Nutzung eines Online-Dienstes oder die eines Kfz-Dienstes ist, je nach Datenart einem anderen Regelungsregime unterworfen werden soll. Zu Recht wird darauf verwiesen, dass eine Abstufung nach unterschiedlich schutzwürdigen Datenkategorien in Anbetracht der vielfältigen möglichen Kfz-Anwendungen ohnehin nicht möglich ist.[26] Daher ist es auch kaum überzeugend, die unterschiedliche rechtliche Einordnung der Nutzung von Inhaltsdaten mit einer besonderen Sensibilität dieser Daten zu begründen. Gerade aus Datenschutzperspektive ist vielmehr eine einheitliche Betrachtungsweise geboten, um für einen einheitlichen Sachverhalt auch ein einheitliches Schutzniveau vorzuhalten. Soweit daher ein konkreter Sachverhalt in seinem Schwerpunkt einen Informations- und Kommunikationsdienst i. S. d. TMG darstellt,[27] ist der Sachverhalt als ganzer dem TMG zu unterstellen.

3.3 Standortdaten: TKG?

Egal, ob es um eCall, Car-to-Car-/Car-to-X-Kommunikation, Navigation oder andere Location Based Services geht, Standortdaten spielen bei der Datenverarbeitung im vernetzten Fahrzeug stets eine zentrale Rolle. Die besondere Schutzwürdigkeit von Standortdaten ist unbestritten (Stichwort Bewegungsprofil), was nicht zuletzt in den strengen Vorgaben des § 98 TKG zur Verarbeitung von Standortdaten seinen Niederschlag gefunden hat. § 98 TKG normiert nicht nur einen strikten Erforderlichkeitsgrundsatz hinsichtlich Umfang und Dauer der Verarbeitung von Standortdaten, sondern setzt darüber hinaus für eine Zulässigkeit der Verarbeitung von Standortdaten auch noch voraus, dass diese Daten entweder anonymisiert wurden oder aber die Datenverarbeitung durch eine Einwilligung legitimiert ist.

Fraglich ist allerdings, in welchen Konstellationen die strengen Anforderungen des § 98 TKG beim vernetzten Kfz überhaupt eingreifen. Standortdaten i. S. d. § 98 TKG sind Daten, „die in einem Telekommunikationsnetz oder von einem Telekommunikationsdienst erhoben oder verwendet werden und die den Standort des Endgeräts eines Endnutzers eines öffentlich zugänglichen Telekommunikationsdienstes angeben" (§ 3 Nr. 19 TKG). Einschlägig ist § 98 TKG also etwa dann, wenn der Anbieter eines Telekommunikationsdienstes mittels eines mit dem Fahrzeug verbundenen Smartphones den Fahrzeugstandort ermittelt und diese Standortdaten dann von ihm oder einem Anbieter von Diensten mit Zusatznutzen verwendet werden.[28] Vergleichbar damit ist die Konstellation, dass die Ortung unmittelbar über das Kommunikationsmodul des Fahrzeugs erfolgt (etwa über eine fest verbaute SIM-Karte) und damit das Fahrzeug selbst das „Endgerät" ist. Zu weit geht es demgegenüber, jede von diesem „Endgerät" ausgehende Standortinformation auch als Standortdaten i.S.d. § 98 TKG einzustufen, egal ob die Erhebung dieser Standortdaten durch den genutzten Telekommunikationsdienst selbst erfolgt oder nicht.[29]

Unabhängig davon, wie weit oder eng man den Anwendungsbereich des § 98 TKG fassen möchte, muss aber jedenfalls die in der Regelung des § 98 TKG zum Ausdruck kommende Grundwertung des Gesetzgebers berücksichtigt werden, dass Standortdaten besonders schutzwürdige Daten sind und diese nur unter ganz engen Voraussetzungen verarbeitet werden dürfen. Ausgeschlossen ist es daher insbesondere, auf Grundlage der allgemeinen Interessenabwägungsklauseln, wie sie im BDSG normiert sind, eine Verarbeitung von Standortdaten zu legitimieren.[30] Allgemeingültiger Maßstab für jede Verarbeitung von Standortdaten muss darüber hinaus das strikte Verständnis des Erforderlichkeitsgrundsatzes sein, wie es in § 98 TKG normiert ist. Und schließlich sind vor allem auch die strengen Anforderungen, die § 98 TKG für die Zulässigkeit einer Fremdortung aufstellt, zu wahren.

3.4 Erforderlichkeit einer Datenverarbeitung

Gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist eine Datenverarbeitung zulässig, wenn dies „für die Begründung, Durchführung und die Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit den Betroffenen erforderlich ist". Die Regelung setzt Art. 7 lit. b der Datenschutzrichtlinie um, wonach die Verarbeitung personenbezogener Daten zulässig ist, wenn dies für die Erfüllung eines Vertrages oder die Durchfüh-

21 In diesem Sinne *Schulz/Roßnagel/David,* ZD 2012, 510, 512.
22 *Jandt/Roßnagel,* MMR 2011, 637, 639.
23 Vgl. *Buchner,* DuD 2012, 767.
24 Vgl. *Weichert*, a.a.O., S. 288 f.*; Schulz/Roßnagel/David*, ZD 2012, 510, 512.
25 Vgl. dazu *Buchner,* BeckOK § 29 BDSG Rn. 38.
26 *Weichert,* a.a.O., S. 289.
27 Dazu soeben 3.1.
28 Vgl. allgemein zu Standortdaten *Jenny* in Plath, BDSG, § 98 TKG Rn. 3. Wohl auch in diesem Sinne (konkret zu Standortdaten eines Fahrzeugs) *Weichert*, a.a.O., S. 297.
29 So auch *Jenny* in Plath, BDSG, § 98 TKG Rn. 2 f. („ nur solche Angaben, die vom Anbieter eines Telekommunikationsdienstes erhoben und dann von diesem oder einem Anbieter von Diensten mit Zusatznutzen verwendet werden, [kann man] als Standortdaten i.S.d. § 3 Nr. 19 TKG verstehen"); a.A. etwa *Munz* in Taeger/Gabel, BDSG, § 98 TKG Rn. 4 („eine Übermittlung des Standortdaten gerade durch den benutzten Telekommunikationsdienst scheint danach nicht erforderlich zu sein").
30 Vgl. *Weichert*, a.a.O., S. 297.

rung vorvertraglicher Maßnahmen erforderlich ist. Vergleichbare Regelungen finden sich auch in sektorspezifischen Gesetzen wie TMG oder TKG.[31] Mit all diesen Regelungen wird zunächst einmal eine Selbstverständlichkeit normiert: Dass die für die Durchführung eines Schuldverhältnisses erforderliche Datenverarbeitung erlaubt sein muss, folgt schon aus der Natur der Sache.[32]

Für die Zulässigkeit einer Datenverarbeitung auf gesetzlicher Grundlage folgt daraus aber auch: Indem das Gesetz das Ob und Wie einer zulässigen Datenverarbeitung an den jeweiligen Inhalt eines Schuldverhältnisses anknüpft, eröffnet es die Möglichkeit, je nach vertraglich vereinbartem Inhalt des Schuldverhältnisses eine Datenverarbeitung in mehr oder weniger großem Umfang auf eine gesetzliche Erlaubnis zu stützen.[33] Konkret heißt das: Je datenintensiver die vertraglich vereinbarte Zwecksetzung eines Schuldverhältnisses ausfällt, desto mehr Daten dürfen auch verarbeitet werden. Wenn sich zukünftig beim vernetzten Fahrzeug Geschäftsmodelle nicht mehr darauf beschränken werden, schlicht ein Auto als Sache zu verkaufen, sondern zukünftig statt des Autos etwa das multimediale „Fahrererlebnis" oder auch das „Gefahren-Werden" durch autonome Fahrzeuge als die Kernleistung eines Schuldverhältnisses auszumachen ist, so sind dann dementsprechend auch die Grenzen einer gesetzlich zulässigen Datenverarbeitung weiter gezogen.

3.5 Datenverarbeitung zu Beweiszwecken

Je mehr Fahrzeugdaten erhoben und längerfristig gespeichert werden, desto wichtiger wird die Frage, ob und unter welchen Voraussetzungen solcherlei Daten (z.B. Betriebs-, Fehler- oder Wartungsdaten) auch zu Beweiszwecken genutzt werden dürfen, etwa wenn es um die Frage geht, ob ein Schadensfall auf die Fehlerhaftigkeit eines Kraftfahrzeugs oder auf einen Fehler des Fahrers zurückzuführen ist. Datenschutzrechtlich handelt es sich bei einer solchen Nutzung von Fahrzeugdaten auch zu Beweiszwecken um eine Zweckänderung, die entweder gesetzlich erlaubt oder durch eine Einwilligung des Betroffenen gedeckt sein muss.

Als gesetzlicher Erlaubnistatbestand für solch eine Zweckänderung kommt hier in erster Linie § 28 Abs. 1 Satz 1 Nr. 2 BDSG in Betracht.[34] Die Verwendung von Fahrzeugdaten zu Beweiszwecken muss daher also zunächst einmal zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich sein (z. B. das Interesse des Kfz-Herstellers, die Fehlerfreiheit des von ihm produzierten Fahrzeugs zu beweisen). Des Weiteren darf kein Grund zu der Annahme bestehen, dass „das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt". Der Sache nach geht es damit um die Frage nach einer Verhältnismäßigkeit der Zweckänderung.

Im Rahmen dieser Verhältnismäßigkeitsprüfung sind dann die verschiedensten Aspekte zu berücksichtigen:

- Unverhältnismäßig wäre es, wenn die Summe aller Fahrzeugdaten, die potenziell als Beweismittel zur Verfügung stehen, im Ergebnis einer Vollzeitüberwachung von Halter oder Führer eines Fahrzeugs gleichkommen würde.[35]
- Ausschlaggebend für die Verhältnismäßigkeitsprüfung ist auch, ob für den Betroffenen offenkundig und nachvollziehbar ist, welche Fahrzeugdaten später möglicherweise auch zu Beweiszwecken herangezogen werden können.
- Eine Rolle kann im Zuge der Verhältnismäßigkeitsprüfung schließlich auch der Aspekt der prozessualen Waffengleichheit spielen. Wenn sich Hersteller für die Nutzung von Fahrzeugdaten zu Beweiszwecken auf ihr berechtigtes Interesse an einer Wahrheitsfindung im Prozess stützen wollen, so muss gewährleistet sein, dass eine solche Nutzungsmöglichkeit dann nicht nur einseitig zugunsten der Hersteller besteht, sondern ebenso auch dem Halter oder Führer eines Fahrzeugs die Möglichkeit eröffnet ist, zu seinen Gunsten zu Zwecken der Wahrheitsfindung auf die Datenspeicher zugreifen zu können.

4 Einwilligung

Wie sonst bei der Datenverarbeitung werden sich auch beim vernetzten Kfz viele Datenverarbeitungsprozesse mangels einschlägiger gesetzlicher Erlaubnistatbestände auf die Einwilligung des Betroffenen als Legitimationstatbestand stützen müssen. Damit sieht man sich dann wieder der klassischen Herausforderung gegenüber, die seit jeher mit der Einwilligung als datenschutzrechtlichem Erlaubnistatbestand verbunden ist: Sicherzustellen ist, dass sich diese Einwilligung nicht in einem bloßen Formalismus erschöpft, sondern tatsächlich ein Ausdruck privatautonomer Selbstbestimmung über den Umgang mit personenbezogenen Daten ist.

Letzteres ist wiederum nur dann der Fall, wenn die rechtlichen Voraussetzungen für eine wirksame Einwilligung erfüllt sind: Es muss gewährleistet sein, dass die Einwilligung bewusst erteilt worden ist. Es muss sich um eine bestimmte und informierte Einwilligung handeln und die Einwilligung muss auf einer freien Entscheidung des Betroffenen beruhen. All diese rechtlichen Anforderungen sind seit jeher bekannt und an sich auch unumstritten. Andererseits zeigen auch hier die Erfahrungen aus der Online-Welt, dass diese Anforderungen in der Praxis immer wieder mehr oder weniger ignoriert werden. Exemplarisch sei auch hier nochmals auf den Fall Facebook verwiesen, wenn sich der Betroffene durch ein simples Klicken auf „Registrieren" im Sinne eines *take it or leave it* pauschal mit jeder nur denkbaren Form einer Datenverarbeitung einverstanden erklären muss, ohne dass ihm der Umstand eines solchen Einwilligens bewusst gemacht wird oder er nachvollziehbar über die Rahmenbedingungen der Datenverarbeitung aufgeklärt wird. Wollte man diese Form der Pro-Forma-Einwilligung genügen lassen und auch für das vernetzte Kfz übernehmen, so würde es dementsprechend ausreichen, wenn auf der Kfz-Bedieneinheit eine Meldung erscheint wie „Indem du auf ‚Fahren' klickst, erklärst du dich mit unseren AGBs und Datenverwendungsrichtlinien einverstanden" (inklusive Verlinkung zu diesen AGBs und Richtlinien).

Jedoch ist eine solche datenschutzrechtliche Praxis weder erstrebenswert noch steht zu erwarten, dass sie langfristig rechtlich Bestand haben wird. Für das sog. „App-Zentrum" von Facebook

31 Siehe etwa § 14 Abs. 1, § 15, Abs. 1 Satz 1, Abs. 5 Satz 1 TMG, § 95 Abs. 1 Satz 1, § 96 Abs. 1 TKG.

32 Vgl. *Tinnefeld/Buchner/Petri,* a.a.O., S. 364.

33 Siehe dazu *Simitis* in ders., BDSG, § 28 Rn. 69 ff.

34 Siehe den Verweis in § 28 Abs. 2 Nr. 1 BDSG. Vgl. dazu *Pötters/Wybitul,* NJW 2014, 2074, 2076 f.

35 Vgl. insoweit auch die Entscheidung des BGH zur Rechtswidrigkeit der Erstellung eines umfassenden personenbezogenen Bewegungsprofils mittels GPS, wenn stattdessen auch eine punktuelle persönliche Beobachtung ausreichend gewesen wäre; BGH DuD 2013, 666.

hat das Landgericht Berlin erst vor kurzem festgestellt, dass simple Anklick-Lösungen in Form eines „Jetzt spielen“[36] nicht ausreichen, um dem Erfordernis einer freiwilligen, zweckbestimmten und informierten Einwilligung ausreichend Rechnung zu tragen.[37] Daran hat auch der Umstand nichts geändert, dass sich die Einwilligung in dem App-Zentrum nicht allein auf das Erfordernis eines Anklickens des Buttons „Jetzt spielen“ beschränkt, sondern auf den Bildschirmen darüber hinaus auch die (Kurz-)Information präsentiert wird, dass es durch das Anklicken zu einer Vielzahl von Datenübermittlungen an dritte Anbieter kommt, sowie darüber hinaus am Ende des Textes sich Links zu AGB und Privacy Policies finden. Das LG Berlin hat insoweit ausdrücklich festgehalten, dass allein auf dieser Informationsgrundlage es weiterhin „völlig offen“ bleibe, welche Daten übermittelt würden, welchem Zweck die Übermittlung dieser Daten diene und was bei Dritten mit diesen Daten geschehe. Eine Verlinkung auf AGBs und Datenschutzbestimmungen genüge gerade nicht, „um dem Nutzer die Tragweite seiner Entscheidung vor Augen zu führen.“ Und es sei auch „nicht ernsthaft damit zu rechnen, dass der durchschnittlich aufmerksame Referenzverbraucher sich vor der Betätigung des Buttons ‚Jetzt spielen‘ noch mühsam durch das Klauselwerk des Spieleanbieters klickt“.[38]

So überzeugend diese Ausführungen des LG Berlin sind, so hoch setzen sie auch die Anforderungen an, die für die Wirksamkeit einer datenschutzrechtlichen Einwilligung zu erfüllen sind – egal ob es um eine Einwilligung in der Online-Welt oder um eine Einwilligung beim vernetzten Kfz geht. Lösungsansätze sind hier viel stärker als bisher bei Instrumenten wie *Privacy by Design* zu suchen. Mehr Transparenz versprechen etwa mehrschichtige Informationsangebote, die situationsbezogen und jeweils nur im Rahmen des Erforderlichen präsentiert werden. Auch bietet es sich an, verstärkt auf Mittel wie Icons oder Tonsignale für eine datenschutz- und nutzerfreundliche Einwilligungseinholung zu setzen.[39] Und schließlich sollte auch darauf geachtet werden, den Nutzer in regelmäßigen Abständen an eine einmal erteilte Einwilligung zu erinnern bzw. sich diese in regelmäßigen Abständen erneuern zu lassen.[40]

5 Fazit

Gerade der letztgenannte Aspekt der Einwilligung macht deutlich, welche datenschutzrechtlichen Herausforderungen zu meistern sind, um die Datenverarbeitung im vernetzten Kfz rechtskonform zu gestalten. Gleichzeitig liegt in diesen Herausforderungen aber auch die eingangs angesprochene Chance für den Datenschutz. Gelingt es, für das vernetzte Fahrzeug den Prozess der Datenverarbeitung so zu gestalten, dass dieser im Unterschied zur Praxis der Datenverarbeitung in der Online-Welt tatsächlich rechtskonform und nutzerfreundlich ist, so kann der Datenschutz im vernetzten Fahrzeug in vielerlei Hinsicht auch eine Vorreiter- und Schlüsselrolle für die Entwicklung des Datenschutzes in Recht und Praxis ganz allgemein einnehmen.

36 Übertragen auf das vernetzte Kfz dann entsprechend „Jetzt fahren“.

37 LG Berlin DuD 2015, 259.

38 LG Berlin DuD 2015, 259, 260.

39 Siehe zu all diesen Lösungsansätzen *Weichert*, a.a.O., S. 300 ff., sowie die Beispiele im Beitrag von *Rieß/Greß* (in diesem Heft).

40 Siehe dazu auch Art. 29 Datenschutzgruppe WP185 – Stellungnahme 13/2011 zu den Geolokalisierungsdiensten von intelligenten mobilen Endgeräten, S. 17.